Security in Software Applications
Third Project

A.A. 2022/2023

The purpose of this project is to experiment with fuzz testing, maybe (but not required) with the code instrumentation Asan (`https://github.com/google/sanitizers/wiki/AddressSanitizer`).

It is recommended the use of afl (`http://lcamtuf.coredump.cx/afl`), a leading tool.

The software to test is the image manipulation software ImageMagick (`https://imagemagick.org/index.php`)- *not the latest release if you want better chances to find vulnerabilities*

(If necessary, other open-source software developed in C can be proposed– but it must be approved first).

Select one of the formats supported (PNG, JPEG, GIF, TIFF, PDF, SVG) to test the application. In the final report (submitted as a single pdf file) you should include

- A few words on the difficulty in setting up the tool
- A brief description of the tool or combination tool/sanitizer
- Summarize the results of your experiments
  - Number of files used o Number of mutations generated
  - Time needed
  - Number of flaws found
  - Are the flaws found known CVEs?

WARNING: Do not open the input files generated by the fuzzer. The effect could be the damaging of the rendering app and of other files that it uses.